

REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 1-22 and 24-32 are pending in the application. Claim 23 is cancelled. Claims 1, 4-7, 10-15, 17, 27, 28, 31, and 32 are amended by the present amendment. Support for the amended Claims can be found in the original specification, claims and drawings. Thus, no new matter is presented.

Turning to the rejections, Claim 23 stands rejected under 35 U.S.C. § 112 as being indefinite. Specifically, the Office Action states that with regard to the “range of validity,” that it is unclear how the range is determined or defined. Applicant respectfully traverses this rejection, but cancels Claim 23 in order to incorporate the range of validity into the independent claims.

As the Office Action correctly points out, paras. 0158 and 0215 of US 2004/0187009 state that the range of validity refers to the extent to which the ticket is valid for authentication purposes. For example, authentication could be valid only in a predetermined domain, system, or server.¹ The rejection appears to center around the claims not explicitly requiring a specific range of validity. Applicant submits that the range of validity limitation is intentionally left broad. This language is intended to cover various embodiments using differing ranges of validity. The range of validity will accordingly depend on the particular application to which the invention is applied. For example in some circumstances an authorization will need to have a very narrow range of validity limiting a user to access only a single server, whereas in other cases, it may be necessary to allow the user much broader access. Therefore, Applicant respectfully submits that further defining of the range of

¹ US 2004/0187009 paras. 0163 and 0216

validity is unnecessary and would unfairly force Applicant to limit the invention where further limitation is not required to clearly define the invention.

With regards to the outstanding Official Action, Claims 1-19, 24, 25, and 27-32 were rejected under 35 U.S.C. § 102(b) as being unpatentable over Gennaro et al. (U.S. Patent No. 6,317,834, herein "Gennaro"). Applicant respectfully submits that amended independent Claims 1, 7, 10, 12, 27 and 31 recite novel features clearly not taught or rendered obvious by the applied reference.

Specifically, Claims 1, 7, 10, 12, 27, and 31 relate to an information providing device, method, and a computer program embodied in a recording medium and a user authentication device, method, and a computer program embodied in a recording medium with a plurality of associated authenticating units which provide a first authentication of the user, and a second authentication of the user based on the information provided during the first authentication. Each of the independent claims are currently amended to add the limitation that *the second authorization only occurs when the user attempts to access something that is not within the limited range of validity*, as discussed above, of the first authorization. For example, the first authorization unit could perform a password authentication which provides limited access, and a fingerprint authentication could additionally be required for full access.² By using a primary provider (such as the password authenticator) and an additional provider (such as the fingerprint authenticator), the user can be given only the minimum necessary amount of authorization for the particular level of access required by the user.³ By so limiting full access to only those situations where it is actually required, circumstances where full access could be improperly obtained by an unauthorized user are reduced significantly.⁴

² Id. at 0064-066

³ Id. at 0088 and 0158-160

⁴ Id. at 0162

Thus, the claimed invention is characterized by the way the biometric user authentication (by fingerprint) and the normal user authentication (by user ID and password) are combined. Specifically, the claimed invention provides the following capabilities:

1) the claimed invention is able to separate the phase in which the normal user authentication is performed by receiving the password from the user, and the phase in which the biometric user authentication is performed as a supplementary authentication by receiving the fingerprint from the user;

2) an application program is not needed to handle an authentication ticket obtained as a result of the password authentication and an updated authentication ticket obtained as a result of the supplementary authentication in a different manner; and

3) the application program is able to detect whether the ticket concerned is an authentication ticket obtained as a result of the supplementary authentication, by making an inquiry to the server as an additional measure. It is possible to change the policy such as access control, by making use of the detection of the ticket.

Turning to the applied reference, Gennaro describes a user authentication method (Fig. 4B) which uses a user identifier 28, a password 30, and a biometric sample 32 to grant a user 26 access to a database. The authorization occurs in the following manner: The user 26 is prompted to enter the personal identifier 28. If the identifier 28 matches one in the system, an encrypted biometric record 33 is retrieved. Then the user 26 is prompted to provide a password 30. The password 30 is then used to create a decryption key 31, which in turn is used to decrypt the encrypted biometric record 33. The user 26 is then prompted to submit a biometric sample 32. Finally, the submitted biometric sample 32 is compared to the decrypted biometric record 40, and a sufficiently high statistical equivalence results in granting the user 26 access to the database.

Accordingly, Gennaro does not describe a situation in which only one authentication procedure is needed. Rather, Gennaro uses multiple forms of authentication to grant a user access. This is because Gennaro contemplates a single level of authorization, and such authorization provides full access to the database. Accordingly Gennaro does not teach a second authorization that only occurs when the user attempts to access something that is not within a limited range of validity associated with the first authorization. Therefore, Applicant respectfully submits that the rejections of Claims 1-19, 24, 25, and 27-32 are overcome by the amendment.

With further regards to the outstanding Official Action, Claims 20-23 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Gennaro in view of Shigematsu et. al. (U.S. Patent Publication No. 2002/0095588, herein “Shigematsu”). Applicant respectfully submits that Claims 20-23 recite novel features clearly not taught or rendered obvious by the applied references.

Claims 20-23 relate to specific details with regard to tickets, which are electronic certificates proving the user is authenticated.⁵ Claim 23 is no longer at issue because it is now cancelled. The remaining claims relate to ticket encoding, terms of validity for tickets, and checking for ticket falsification.

Turning to the additionally applied reference, Shigematsu describes a user authentication token and system. A physical authentication token 1 is connected to a use device 2 which the user is attempting to operate. The user places a finger on the sensor 11, and assuming it matches the stored record, the token outputs the user ID, password, and personal information stored in the storage circuit 12 in the form of authentication data 13A.

First, Applicant submits that the rejection of Claims 20-23 are overcome for the reasons set forth above due to their dependence on amended independent Claim 12. This is

⁵ Id. at 0151

because Shigematsu additionally fails to disclose a multi-tiered authorization system as now claimed. Rather, Shigematsu teaches sending all of the authentication data 13A at one time.⁶ Further, Applicant submits that the limitations of Claim 21 are not met because neither Gennaro nor Shigematsu teaches a term of validity for electronic tickets (i.e. the tickets are only valid for a certain period of time⁷). Rather, it appears that both applied references teach authentication for an unlimited duration.

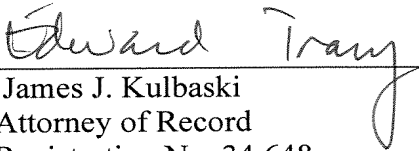
With further regards to the outstanding Official Action, Claim 26 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Gennaro. Applicant submits that the rejection of Claim 26 is overcome for the reasons set forth above due Claim 26's dependence on amended independent Claim 12.

With respect to the remaining amendments, Claims 4-6, 11, 13-15, 17, 28, and 32 are currently amended to correct spelling errors and provide greater clarity.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1-22 and 24-32 is definite and patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.


James J. Kulbaski
Attorney of Record
Registration No. 34,648

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

Andrew T. Harry
Registration No. 56,959

I:\ATTY\ATH\PROSECUTION\25'S\250627US\250627US - REVISED AM DUE 092507.DOC

⁶ US 2002/0095588 para. 0073

⁷ US 2004/0187009 para. 0156

Edward W. Tracy
Registration No. 47,998